Government of Canada | Gouvernement du Canada

UPDATE REPORT ON

DEVELOPMENTS IN DATA PROTECTION LAW IN CANADA (2001-2017)

Report to the European Commission May 2017

Canada

This publication is available online at http://www.ic.gc.ca/eic/site/iccat.nsf/eng/07392.html.

To obtain a copy of this publication, or to receive it in an alternate format (Braille, large print, etc.), please fill out the Publication Request Form at www.ic.gc.ca/Publication-Request or contact:

Web Services Centre
Innovation, Science and Economic Development Canada
C.D. Howe Building
235 Queen Street
Ottawa, ON K1A 0H5
Canada

Telephone (toll-free in Canada): 1-800-328-6189
Telephone (international): 613-954-5031
TTY (for hearing impaired): 1-866-694-8389
Business hours: 8:30 a.m. to 5:00 p.m. (Eastern Time)
Email: ISED@canada.ca

Permission to Reproduce

Except as otherwise specifically noted, the information in this publication may be reproduced, in part or in whole and by any means, without charge or further permission from the Department of Industry, provided that due diligence is exercised in ensuring the accuracy
of the information reproduced; that the Department of Industry is identified as the source institution; and that the reproduction is not represented as an official version of the information reproduced or as having been made in affiliation with,
or with the endorsement of, the Department of Industry.

For permission to reproduce the information in this publication for commercial purposes, please fill out the Application for Crown Copyright Clearance at www.ic.gc.ca/copyright-request or contact the Web Services Centre mentioned above.

© Her Majesty the Queen in Right of Canada, as represented by the Minister of Industry, (2018).

Cat. No. Iu37-8/2018E-PDF
ISBN 978-0-660-25849-2

Aussi offert en français sous le titre *Rapport d'étape sur les évolutions en matière de législation sur la protection des données au Canada (2001-2017)*

Table of Contents

1.0 Introduction 4

2.0 The Canadian Context 4

3.0 Canada's private sector privacy law (PIPEDA) 5

4.0 Canada's public sector privacy law (Privacy Act) 9

5.0 Canadian Charter of Rights and Freedoms 11

6.0 Access for law enforcement and national security purposes 12

7.0 Recent Developments 16

8.0 Further Information and Reports 17

1. 0 Introduction

1.1. On December 20, 2001, the European Commission (EC) issued Decision 2002/2/EC, pursuant to Article 25(6) of Directive 95/46/EC (hereinafter "the Directive"). The Decision states that Canada is considered as providing an adequate level of protection of personal data transferred from the European Union (EU) to recipients subject to the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

1.2. This decision allows EU operators to send certain personal data to recipients in Canada subject to PIPEDA without additional safeguards being needed to meet the requirements of the Directive.

1.3. In Implementing Decision (EU) 2016/2295 of December 16, 2016, the EC amended Decision 2002/2/EC to conform to the judgement of the Court of Justice of the European Union of October 6, 2015 in Case C-362/14 Maximillian Schrems v Data Protection Commissioner.

1.4. In accordance with Article 2 of Implementing Decision (EU) 2016/2295, the EC is now required, on an ongoing basis, to monitor developments in the Canadian legal order, including developments concerning access to personal data by public authorities, with a view to assessing whether Canada continues to ensure an adequate level of protection of personal data.

1.5. In a letter dated January 25, 2017, the EC's Directorate-General for Justice and Consumers invited Canada to assist the Commission with its monitoring obligations by providing information on any material changes or developments related to privacy and data protection since Decision 2002/2/EC. The correspondence also requested information on the limitations and safeguards regarding access to personal data by public authorities in Canada, particularly for national security and law enforcement purposes.

1.6. With a view to assisting the Commission in its monitoring obligations under Implementing Decision (EU) 2016/2295, the following draft report outlines:

- developments in Canada's data protection framework applicable to private sector organizations and government entities, and
- information on the limitations and safeguards governing the access to personal data by public authorities, particularly for national security and law enforcement purposes.

2.0 The Canadian Context

2.1 In Canada, the *Canadian Charter of Rights and Freedoms ("the Charter")* is a fundamental law that provides constitutional protection for human rights. This includes the right to life, liberty and security of the person under section 7, the right to be free from unreasonable searches and seizures under section 8, and equality before and under the law under section 15. All laws and government actions at both the federal and provincial levels must conform to the Charter, which can be enforced by the courts. As a part of Canada's Constitution, the *Charter* takes precedence over other laws and sets limits on government action.

2.2 At the federal level, Canada's privacy framework includes two central privacy statutes. The *Personal Information Protection and Electronic Documents Act* (PIPEDA)[1] provides the basic legal framework for the private sector, setting out how companies are to protect and manage personal information in the context of commercial activities. The *Privacy Act* provides the basic legal framework for the collection, retention, use and disclosure of personal information by government institutions.

2.3 All government activity, whether authorized by statute or by common law, are subject to the restrictions in the *Charter*. In addition, Government treatment of personal information is always subject to a framework of public sector laws. Some of these laws provide specific authorities for government to collect, use, retain or disclose personal information for particular purposes.

2.4 The independent judiciary provides jurisprudence interpreting government authorities and civil rights. Individuals have access to specialized oversight mechanisms such as the Office of the Privacy Commissioner of Canada, the Office of the Auditor General of Canada, as well as the several bodies that review the actions of core national security agencies (e.g. the Security Intelligence Review Committee, and the Civilian Review and Complaints Commission of the Royal Canadian Mounted Police).

2.5 Government departments are required to exercise their legal authorities in accordance with policies and guidelines established by the President of Treasury Board, as designated Minister, and in compliance with regulations, if any are promulgated under statutes.

2.6 In Canada's legal system, decisions of courts on matters of public law are considered binding precedents that must be followed by future instances of courts, and by officials charged with applying the law. As a result, over time, courts develop binding interpretations of legislative text that are often more restrictive than what the apparently broad language of a statute might suggest. These interpretations are influenced by both the common-law principle that laws that have the effect of limiting rights tend to be interpreted restrictively, and that interpretation should be informed by the *Charter*. Canadian legislation must therefore be read in conjunction with applicable jurisprudence in order to ascertain the true effect of a given provision.

2.7 In short, Canada features a data protection framework governing the private sector and also a framework governing the public sector which are best understood in light of the Canadian legal system where activities of government are subject to the Rule of Law, requirements of reasonableness, compliance with balanced statutory limits, oversight institutions and internal compliance mechanisms.

3.0 Canada's Private Sector Privacy Law (PIPEDA)

3.1 The *Personal Information Protection and Electronic Documents* (PIPEDA) is Canada's federal statute for privacy and data protection in the private sector and establishes legal equivalence for electronic documents. Part I of the Act sets the legal requirements for the protection of personal information in Canada. It applies to every organization that collects uses or discloses personal information in the course of commercial activities. The Act does not apply to public sector organizations, which are governed by the *Privacy Act,* or to those that are regulated by the public sector at the provincial level. PIPEDA sets limits on the collection, use and disclosure of personal information by organizations. It also

[1] Canadian federal statutes are available at http://laws.justice.gc.ca/eng/

sets out limited and specific conditions under which organizations disclose personal information to government institutions and law enforcement. Enforcement of PIPEDA relies on an ombudsman model, with oversight and redress mechanisms provided through the Office of the Privacy Commissioner of Canada (OPC) and the Federal Court. The OPC operates as the federal data protection authority with the mandate to protect and promote the privacy rights of individuals.

3.2 PIPEDA came into force on January 1, 2001 and is recognized as an advanced and well respected privacy regime. The Act balances the individual's right to privacy with the need of organizations to collect, use or disclose information for legitimate business purposes. It is based on a set of ten privacy principles[2] that have stood the test of time. Like the OECD Privacy Guidelines[3] on which it was based, PIPEDA is a principles-based framework that has remained intact with legislative amendments made to only specific aspects to improve its effectiveness.

Substantially Similar

3.3 In order to facilitate the development of harmonized federal and provincial privacy laws, PIPEDA includes a provision allowing for provincial statutes to be deemed "substantially similar" under the Act. A formal process for the determination of substantially similar laws has been established whereby laws are deemed substantially similar to PIPEDA if they "provide privacy protection that is consistent with and equivalent to that found under PIPEDA, incorporate the ten principles in Schedule 1 of PIPEDA, provide for an independent and effective oversight and redress mechanism with powers to investigate, and restrict the collection, use and disclosure of personal information to purposes that are appropriate or legitimate."

3.4 Provinces with such legislation are exempt from PIPEDA which allows for the collection, use or disclosure of personal information to be governed by provincial law. However, PIPEDA continues to apply to the collection, use or disclosure of personal information with respect to federal undertakings and to the collection, use or disclosure of personal information outside of the province. Several provincial laws have been granted the substantially similar designation, applying either generally to personal information holdings of organizations within the province, or to personal health information only.

3.5 Quebec, Alberta and British Columbia have passed their own private sector privacy laws. Quebec's law was deemed substantially similar to PIPEDA in 2003 with Alberta and British Columbia's laws being recognized in 2004. Health sector privacy laws have been passed in Ontario, New Brunswick, Newfoundland and Labrador, and Nova Scotia and were deemed substantially similar to PIPEDA in 2005, 2011, 2012 and 2016 respectively.

Statutory Review of PIPEDA

3.6 A statutory review of the Act is required every five years by parliamentary committee. The first statutory review of PIPEDA resulted in the passage of The Digital Privacy Act in 2015. While the Bill received Royal Assent on June 18, 2015, the new regime for mandatory data breach notification, forming Division 1.1 of PIPEDA, will come into force once the Regulations governing data breach incidents are final.

[2] The ten principles in Schedule 1 of PIPEDA are: accountability, identifying purposes, consent, limiting collection, limiting use, disclosure and retention, accuracy, safeguards, openness, individual access and challenging compliance.
[3] 2013 OECD Privacy Guidelines at https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm

The Digital Privacy Act (2015)

3.7 The Digital Privacy Act (2015) amended PIPEDA in three substantive ways by adding:

- measures to protect consumers;
- provisions related to exceptions to consent; and
- measures to increase compliance.

Protecting Consumers

3.8 *New Division 1.1 on Data Breach Notification:* The 2015 amendments introduced a new Division to the Act entitled "Breaches of Security Safeguards" which sets out mandatory notification requirements for organizations when personal information has been compromised due to a breach of security safeguards resulting in a "real risk of significant harm to the individual". Organizations will be required to report data breaches involving personal information to the Privacy Commissioner of Canada and to notify affected individuals. These changes will empower consumers and encourage businesses to improve information security practices.

3.9 *Record Keeping for Data Breaches:* Organizations will be required to keep and maintain a record of every breach of security safeguard involving personal information under their control and provide the record to the Privacy Commissioner upon request. This will allow the Privacy Commissioner to fulfill the required oversight role and make sure that companies are reporting potentially harmful breaches.

3.10 *Enhanced Consent*: There are new requirements for obtaining consent for the collection, use or disclosure of personal information designed to protect vulnerable individuals, especially children. The new consent requirements ensure that when organizations seek to collect personal information, they clearly communicate the purpose in a way that is easily understood by their target users.

Exceptions to Consent

3.11 *Public interest:* There are new provisions to clarify situations where, for reasons of public interest, organizations are allowed to disclose personal information without the knowledge or consent of the individual. These include: i) identifying an injured, ill or deceased individual and communicating with their next of kin; ii) preventing, detecting or suppressing fraud; and iii) protecting victims of financial abuse.

3.12 *Information Sharing:* There are changes to section 7 of the Act with respect to disclosure of personal information between organizations without the knowledge and consent of the individual. Previously, information sharing between organizations was governed by an investigative bodies regime, where organizations designated under the Act as an investigative body were able to disclose personal information to other investigative bodies. This regime has been repealed and replaced with specific circumstances under which information can be shared. These include disclosures for the purposes of investigating a breach of agreement, contravention of law, or for detecting, suppressing or preventing fraud.

3.13 *Specific Business Activities:* There are new provisions to indicate that organizations are not allowed to collect, use and disclose personal information, without the knowledge or consent of an individual, except when it is necessary to support specific and legitimate business activities. This includes information that is:

- produced by the individual in the course of their employment, business or profession (work product);
- related to prospective or completed business transactions such as acquisitions;
- needed to establish, manage or terminate their employment relationships with the individual; or
- contained in witness statements related to insurance claims.

Increased Compliance

3.14 *New Compliance Agreements*: Section 17.1 of the Act includes new provisions for the Office of the Privacy Commissioner to enter into a compliance agreement with an organization to ensure compliance with the Act. This new regulatory tool provides an alternative to Court action or penalties when an organization has been found to be in contravention with a legal obligation under the Act. These agreements enable organizations to make a binding commitment to take action to ensure compliance with the Act and avoid costly legal action. At the same time, they allow the Commissioner to hold organizations accountable when they fail to protect their customers.

3.15 *Increased time for Application to the Courts:* There are new provisions that extend the period within which a complainant may apply to the Federal Court of Canada for a hearing. Complainants, including the Commissioner, have up to a year after an investigation has been completed to ask the Federal Court to order an organization to comply with the law or to award damages to an individual who has been harmed as the result of a privacy violation. This allows more time for an organization to voluntarily take corrective action or negotiate a compliance agreement.

3.16 *Additional Fines and Penalties:* New offences were created for deliberately failing to report a data breach to the Commissioner or to an individual, or for deliberately failing to maintain, or destroying data breach records. These offences are subject to a fine of up to $10,000 on summary conviction, and up to $100,000 on indictment.

Other Developments

3.17 *Addition of Schedule 4:* PIPEDA was amended in 2015 to specify that the Act applies to the World Anti-Doping Agency (WADA).[4] Subsection 4(1.1) was added to PIPEDA along with a new Schedule (Schedule 4) for the purpose of listing WADA and other organizations.

Consequential Amendments to PIPEDA

3.18 There are four instances where PIPEDA was amended as a consequence of other legislative initiatives in Canada. The introduction of Canada's new anti-spam law in 2014, the strengthening of the *Public Servants Disclosure Protection Act* in 2005, amendments to the *Public Safety Act* in 2004, and the introduction of The *Anti-terrorism Act* which came into force in December 2001, all included consequential amendments to PIPEDA. The four legislative amendments are described below.

3.19 *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities*, more commonly referred to as Canada's Anti-Spam Law (CASL), came into force on July 1, 2014. CASL included consequential amendments to section 7 of PIPEDA to introduce new definitions relating to electronic addresses. It also introduced several new provisions to

[4] WADA is an international organization headquartered in Canada (Montreal), tasked with promoting, coordinating and monitoring the fight against the illegal use of drugs in sport.

PIPEDA related to contraventions, new discretionary powers for the Privacy Commissioner, the Commissioner's powers to work in coordination with provincial/territorial commissioners, and to share information about investigations with foreign counterparts.

3.20 In November 2005, the *Public Servants Disclosure Protection Act* came into force. The Act includes consequential amendments to PIPEDA; notably clause 57 of the Act amends section 9(3) of PIPEDA and functions as a means to protect the identity of whistleblowers. In addition, a discretionary exemption was added to PIPEDA to refuse to disclose personal information where a formal request for access has been filed. This amendment was added to "further strengthen the protection of the identity of parties in wrongdoing disclosures made within organizations".

3.21 *An Act to amend certain Acts of Canada, and to enact measures for implementing the Biological and Toxin Weapons Convention, in order to enhance public safety*, more commonly known as the *Public Safety Act, 2002*, came into force on May 6, 2004. Section 7 of PIPEDA was amended to permit the collection and use of personal information for reasons of national security, the defence of Canada or the conduct of international affairs, or when the disclosure of the information is required by law. The amendment clarified that organizations subject to PIPEDA have the authority to collect and use information about individuals without their knowledge or consent for the purpose of making such disclosures. Section 7 of PIPEDA underwent subsequent amendment under The Digital Privacy Act of 2015 as noted above.

3.22 The *Anti-terrorism Act* came into force on December 18, 2001. Consequential amendments to subsections 7(3) and 9(2.3) of PIPEDA were made that pertain to *the Proceeds of Crime (Money Laundering) Act*. PIPEDA was further amended to accord with provisions of the *Canada Evidence Act* which affect transparency and access of individuals to their personal information and address the "judicial balancing of interests between the public interest in disclosure and the interest of the state in national security and maintaining foreign confidences."

4.0 Canada's public sector privacy law (*Privacy Act*)

4.1 The *Privacy Act* applies to all federal government departments and most agencies, as well as Crown corporations and their wholly-owned subsidiaries. It limits the collection of personal information by government institutions to personal information that relates directly to their programs or activities. The Act requires government institutions to collect personal information for administrative purposes directly from individuals, wherever possible, and to inform those individuals of the purpose of this collection. It also requires government institutions to use personal information for the purpose of its collection, for a use consistent with that purpose, with the consent of the individual to whom the information relates, or for purposes for which the personal information may be disclosed under the Act.

4.2 The Act allows government institutions to disclose personal information with the consent of the individual to whom it relates, or in accordance with a limited set of disclosure permissions set out in the Act. It sets rules on how government institutions must retain certain personal information after its use, and how they must dispose of it. The Act gives Canadian citizens, permanent residents and those present in Canada the right to request personal information that government institutions hold about them, subject to exemptions and exclusions. It also creates transparency requirements for government's treatment of personal information. For example, the Act requires that government institutions maintain personal information banks which include descriptions of personal information under their control

which has been used, is being used, or is available to be used for an administrative purpose. The Act requires the President of the Treasury Board to publish these personal information banks, which are accessible to the public through the following website: https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/access-information/information-about-programs-information-holdings.html.

4.3 The *Privacy Act* is one element of the overall public sector privacy regime in Canada. Depending on the government function – and the types of information – more specific rules may be found in other federal statutes and regulations. To take just a few examples: Part 4 of the *Department of Employment and Social Development Canada Act* contains specific rules relating to personal information used in administering important social and income support programs; section 241 of the *Income Tax Act* restricts the treatment of taxpayer information; and sections 17 and 18 of the *Statistics Act* restricts disclosure of census information.

4.4 The *Privacy Act* also establishes the Office of the Privacy Commissioner of Canada. The Commissioner is an independent ombudsman with powers to investigate complaints, make recommendations respecting compliance with the Act, and issue reports to Parliament. The Act creates a right to apply to the Federal Court in respect of a refusal to provide an individual who has access rights under the Act with access to their personal information.

4.5 The Privacy Commissioner of Canada recognizes that, with an appropriate agency arrangement with a person present in Canada, any individual, including non-Canadians outside of Canada, may ask their agent to make a request for information under the *Privacy Act* and authorize the disclosure of their own personal information to their agent[5]. The Act also allows the Commissioner to receive and investigate complaints submitted by authorized representatives and enables authorized representatives to exercise access-related rights of judicial review set out therein. Additionally, "anyone directly affected" by the collection, use or disclosure of personal information, may challenge the lawfulness of government action through judicial review under section 18.1 of the *Federal Courts Act*.

4.6 *Policies relating to the Privacy Act* - The President of the Treasury Board of Canada has issued several government-wide policies which apply to all federal government institutions subject to the *Privacy Act* and support its administration across the government. This includes the *Policy on Privacy Protection*,[6] which sets out requirements regarding the application of the *Privacy Act* and its Regulations. Associated with this policy instrument is a series of Directives[7] which set out requirements related to the management of personal information, the creation of privacy impact assessments which identify privacy implications for new or substantially modified programs and activities, requests for personal information that government institutions hold or correction of that information, restrictions on the use of the social insurance number, as well as a number of guidelines dealing with privacy breaches, information sharing agreements, and contracting decisions.

---

[5] Office of the Privacy Commissioner's Website (https://www.priv.gc.ca/en/privacy-topics/access-to-personal-information/accessing-your-personal-information/)

[6] *Policy on Privacy Protection* (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12510)

[7] *Directive on Privacy Practices* https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18309 ;
Directive on Privacy Impact Assessments https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308 ;
Directive on Privacy Requests and Correction of Personal Information https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18311 ;
Directive on Social Insurance Number https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=13342 ;
Guidance on Preparing Information Sharing Agreements Involving Personal Information https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html ;
Guidance Document: Taking Privacy into Account Before Making Contracting Decisions https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-document-taking-privacy-into-account-before-making-contracting-decisions.html ;
Guidelines for Privacy Breaches https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26154

Law Reform of the *Privacy Act*

4.7 In March 2016, the House of Commons' Standing Committee on Access to Information, Privacy and Ethics (ETHI) launched a study of the *Privacy Act*. On November 24, 2016, the Minister of Justice announced to the ETHI Committee that she was leading a review towards modernizing the *Privacy Act* with the support of the President of the Treasury Board and other colleagues. The Department of Justice Canada is leading this interdepartmental law review work of the *Privacy Act*, which includes examination of the recommendations contained in the Report issued by the ETHI Committee on December 12, 2016.[8]

5.0 The *Canadian Charter of Rights and Freedoms*

5.1 The *Canadian Charter of Rights and Freedoms* protects privacy rights through section 8, which guarantees that "everyone has the right to be secure against unreasonable search[9] or seizure". This provision can be described as playing a role in Canada's legal framework similar in some ways to that of Article 7 of the *Charter of Fundamental Rights of the European Union*, Article 8 of the *European Convention on Human Rights* or the Fourth Amendment to the Constitution of the United States.

5.2 Section 8 of the *Charter* protects against "unreasonable" searches, and so courts must determine whether a search is reasonable in order to determine whether it infringes section 8. In order for a search to be "reasonable," it must be authorized by law, the law itself must be reasonable, and the search must be carried out in a reasonable manner. For a law authorizing an invasion of privacy to be reasonable, it must strike a proper balance between the interests of society and the rights of individuals. This is a flexible test, and can involve examining, among other things, the nature and the purpose of the legislative scheme, the mechanism employed and the degree of its potential intrusiveness, and the availability of judicial supervision. In the criminal context, section 8 generally requires that searches be authorized in advance by a judicial warrant. In the administrative and regulatory contexts, there is greater scope under the *Charter* for warrantless search powers.

5.3 By imposing a requirement that searches be authorized by reasonable lawful authority, and by allowing courts to invalidate unreasonable laws and to order remedies for unauthorized or unreasonable government invasions of privacy, section 8 of the *Charter* forms an important part of the overall framework for privacy protection in Canada.

5.4 In Canada's legal system, caselaw on public-law matters is treated as legally binding precedent that must be followed by lower courts. The law under section 8 of the *Charter* is therefore constantly evolving as cases are decided. Below are some recent examples of caselaw that may be relevant to the protection of customer data, the first two dealing with the privacy implications of searches involving computers, and the third set dealing generally with searches where the target may not be aware of the search.

5.5 In 2013, in *R. v. Vu*, the Supreme Court of Canada confirmed that a warrant to search a physical location cannot implicitly authorize the searches of electronic devices such as computers found at that location. Because of the significant amounts of personal data that they can contain, computers and similar devices may only be searched if the

[8] This report is available on the website of the Committee: http://www.parl.gc.ca/content/hoc/Committee/421/ETHI/Reports/RP8587799/ethirp04/ethirp04-e.pdf.
[9] For the purposes of section 8 of the *Charter*, a "search" is any state action that intrudes upon a reasonable expectation of privacy. Whether an action engages a reasonable expectation of privacy is determined based on the totality of the circumstances. The protection of section 8 is not limited to physical searches, and encompasses protection for informational privacy.

judge issuing the search warrant has specifically authorized this. That is to say, the judge must be satisfied that there are reasonable grounds to believe[10] that the computer to be searched will afford evidence of an offence.

5.6 In 2014, in *R. v. Spencer*, the Supreme Court of Canada examined whether internet service providers could provide police with the identity of a subscriber associated with the use of a particular Internet Protocol address at a particular time, in response to a non-binding request from police officers. The Court found that the reasonable expectations of privacy enjoyed by internet users included an expectation of anonymity, given that an IP address can, when associated with an identity, reveal highly personal information about an individual. Since the obtaining of subscriber identity information engaged a reasonable expectation of privacy, reasonable lawful authority was required. The court found that subparagraph 7(3)(*c.1*)(ii) of PIPEDA did not constitute lawful authority, as it only allowed organizations to release data to police where the police had lawful authority to acquire it. In other words, police require independent reasonable lawful authority to obtain such information from ISPs.

5.7 On a more general level, several cases in recent years have emphasized the role that the availability of after-the-fact judicial review can play in evaluating the reasonableness of a law that authorizes a search, particularly where the search is one of which the subject may not otherwise become aware. For example, in *R. v. Tse* the Supreme Court of Canada found that provisions of the *Criminal Code* that authorized warrantless wiretaps in exigent circumstances were unreasonable in part because they did not include a mechanism to notify targets that their communications had been intercepted. Notification was found to be necessary to enable the targets of searches to challenge such searches in court and Canada's *Criminal Code* has been amended to include this requirement. On a related note, in *R. v. Fearon* the Court found that thorough record-keeping was required in order to ensure that the reasonableness of a particular type of warrantless search could be properly evaluated by a reviewing court. These are some examples of the flexible approach, described above, that courts apply in determining whether a law authorizing invasions of privacy is "reasonable" and therefore consistent with section 8 of the *Charter*.

6.0 Access for law enforcement and national security purposes

Access for law enforcement purposes

6.1 Primary investigative tools for law enforcement are set out in Canada's *Criminal Code*, including search warrants, preservation demands and orders, and production orders and wiretap authorizations. There are also investigative powers for law enforcement outlined in Canada's *Mutual Legal Assistance in Criminal Matters Act* (*MLACMA*) which is Canada's legislative authority to assist foreign partners in obtaining evidence and other assistance for their criminal investigations and prosecutions. Under the MLACMA, Canada has the ability to obtain court orders on behalf of foreign partners, including search warrants, other warrants, production orders and subpoenas.

6.2 The level of prior judicial authorization required for authority to use certain investigative techniques reflects and is determined by the level of intrusiveness of the respective technique and the reasonable expectation of privacy a person has in the information gathered by the use of the technique.

6.3 *Prior Judicial Authorization* - Investigative techniques that involve search and seizure allowing police and other

[10] "Reasonable grounds to believe" is a recognized standard in Canadian law which requires an objective basis for such a belief, based on compelling and credible information.

law enforcement agencies to obtain information generally require prior judicial authorization where a reasonable expectation of privacy exists, though there are exceptions to this general rule, such as in exigent circumstances. The application for prior authorization is usually heard *ex parte*, which means that the suspect is not represented as involving the suspect at this stage of an investigation would undermine the police's ability to collect evidence and would reveal sensitive investigative techniques.

6.4 Two judicial standards are commonly used in Canada's *Criminal Code*: Reasonable grounds to believe – for information or techniques in relation to which a person has a higher expectation of privacy (i.e., email content); and reasonable grounds to suspect – for information with a reduced expectation of privacy (e.g. telephone numbers dialled) and for less intrusive investigative techniques. Reasonable grounds to believe, or suspect, is a recognized standard in Canadian law which requires an objective basis for believing or suspecting based on compelling and credible information.

6.5 *Warrants and Orders* - Although there are a variety of court processes provided for in the *Criminal Code*, those that relate to investigative techniques can be generally divided into two categories; warrants and authorizations, which authorize state actors, such as law enforcement agents, to do something; and orders, which compel civilians to do something.

6.6 Warrants and authorizations generally authorize the police to do something that would impact upon a person's reasonable expectation of privacy. For example, a search warrant authorizes police to enter a premise and search for evidence of an offence. Production orders, on the other hand, compel a third party to compile documents or data in their possession or control for the purposes of the investigation.

6.7 *Search Warrants* - A search warrant is a tool used by police to conduct a search, including for example a home, computer or car. Because it is a broad search power it is granted once the conditions have been met under the reasonable grounds to believe standard.

6.8 *Tracking Warrants* - A tracking warrant can authorize tracking location of transactions (i.e. credit card records), the location or movement of things (i.e. a vehicle), or the movement of an individual by identifying the location of a thing that is usually carried or worn by the individual (i.e. a cell phone). Warrants for tracking were updated in the *Protecting Canadians from Online Crime Act*, which came into force in March 2015, to address advances in technology, in particular the accuracy of such devices and their potential for increased impact on privacy, by increasing the level of judicial scrutiny required when they apply to the tracking of individuals using a thing usually carried or worn.

6.9 *Transmission Data Recorder Warrants* - The new transmission data[11] recorder warrant, brought into law by the *Protecting Canadians from Online Crime Act*, replaced the old number recorder warrant to make the investigative technique applicable to Internet telecommunications.

6.10 *Wiretap Authorizations* - Since 1974, it has been an offence in Canada to intercept the private communications of another person unless authorized under the *Criminal Code*. Part VI of the *Criminal Code* sets out a number of methods for how police can be authorized to intercept the private communications of Canadians, which intercept includes the content of communications, including through prior judicial authorization and in emergency situations.

[11] Transmission data has been defined to include all data relevant to the transmission of a telecommunication. However it remains as limited as its predecessor in that it does not include the content of the communication, but rather only information about how the communication got from the sender to the recipient of the communication.

6.11 *General Warrant* - A general warrant can be obtained for investigative techniques that are not otherwise provided for by another warrant in the *Criminal Code*. The general warrant can be useful for the police for unique and unusual situations, or new and evolving environments, to seek appropriate prior judicial authorization.

6.12 *Assistance Order* - In support of any warrant or authorization a judge may also issue an assistance order, which compels a third party to provide assistance if it is reasonably considered to be required to give effect to the warrant or authorization.

6.13 *Data Preservation*[12] - Data preservation tools were introduced in the *Criminal Code* by the *Protecting Canadians from Online Crime Act*. These tools prevent computer data from being deleted until a judicially authorized warrant or order for its acquisition can be issued.

6.14 *Production Orders* - Production orders range from orders which can compel comprehensive production of data and documents in relation to which there is a higher expectation of privacy, to orders for specific, less private and limited information. Production orders have been in the *Criminal Code* since 2004, but the *Protecting Canadians from Online Crime Act* added three new low threshold production orders to assist police at the earlier stages of investigations. The new low threshold production orders provide police with tools to collect transmission data, tracking data, and tracing data, which were added to the existing low threshold production order for basic financial data. The data or information that can be obtained at a lower standard using these production orders may be of a personal nature but is not information that is very private or revealing.

6.15 The *Protecting Canadians from Online Crime Act* also amended the *MLACMA* by incorporating the new *Criminal Code* threshold production orders which allow certain data to be gathered on a lower legal threshold. The amendment also created a separate procedural regime for executing Criminal Code tracking warrants and transmission data warrants. It further provides a more streamlined process for sending the fruits of the new production orders and warrants to the foreign partner. These powers form an essential part of Canada's law enforcement toolkit; without the ability to assist foreign partners with their investigations, Canada would not be able to, in turn, seek assistance from them to obtain digital evidence nor would Canada be able to fully participate in the global fight against serious international crime.

Access for national security purposes

6.16 The Canadian Security Intelligence Service (CSIS) is Canada's domestic security intelligence agency. CSIS' role is to investigate activities suspected of constituting threats to the security of Canada, and to report on these to the Government of Canada. Its activities are governed by the *Canadian Security Intelligence Service Act* (CSIS Act), which includes requirements for the collection, use, retention, and disclosure of information. CSIS must also conduct its activities in accordance with the *Privacy Act* and the *Canadian Charter of Rights and Freedoms*.

6.17 *Prior Judicial Authorization* – Prior judicial authorization is required for CSIS to use investigative techniques that engage an individual's reasonable expectation of privacy under section 8 of the *Charter*. The application for prior authorization is heard *ex parte*, which means that the subject of the investigation is not represented. Involving the subject of investigation would be injurious to Canada's national security given that sensitive investigative techniques

[12] In Canada, the term data preservation is not interchangeable with "data retention". The term "data retention" refers to a general obligation which requires service providers to collect and store certain data for a prescribed period of time, for all subscribers, regardless of whether or not they are subject to an investigation. General data retention is not a requirement in Canada.

would be revealed.

6.18 The judicial standard of "reasonable grounds to believe" must be met in order for a judge to issue a warrant under the CSIS Act, and other conditions must be satisfied before the court can issue a warrant under the Act. The judge hearing the application for a warrant must be satisfied on oath by the Director of CSIS, or a designated employee, that, among other things: (1) a warrant is required to investigate a threat to the security of Canada (as defined in section 2 of the CSIS Act)[13]; (2) other investigative procedures have been tried and have failed or are unlikely to succeed; and, (3) the urgency of the matter is such that it would be impractical to carry out the investigation using only other investigative techniques or that it is likely that information of importance with respect to the threat to the security of Canada or the performance of CSIS' mandate to, within Canada, collect foreign intelligence, would be missed without a warrant.

6.19 In addition, the CSIS Act contains several other requirements that frame CSIS activities. For example, CSIS must obtain the approval of the Minister of Public Safety and Emergency Preparedness prior to applying to the Federal Court for a warrant. The Minister also issues direction concerning operational procedures and approves cooperative agreements and relationships with foreign agencies. The CSIS Act also provides for a rigorous system of review by the Security Intelligence Review Committee (SIRC), which has access to all information in the possession of CSIS. SIRC and has a mandate to report annually on CSIS activities to the Parliament of Canada.

6.20 The *Proceeds of Crime (Money Laundering) Act* was amended in December 2001 to become the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA). The objectives of the PCMLTFA are to:

- implement specific measures[14] to detect and deter money laundering and the financing of terrorist activities to facilitate the investigation or prosecution of money laundering and terrorist financing offences;
- respond to the threat posed by organized crime by providing law enforcement officials with the information they need to investigate and prosecute money laundering or terrorist financing offences, while ensuring that appropriate safeguards are put in place to protect the privacy of persons with respect to personal information about themselves; and
- assist in fulfilling Canada's international commitments to participate in the fight against transnational crime, particularly money laundering and the fight against terrorist activities.

6.21 In 2014, the PCMLTFA was further amended to enhance the client identification, record keeping and registration requirements for financial institutions and intermediaries, refer to online casinos, and extend the application of the Act to persons and entities that deal in virtual currencies and foreign money services businesses. Modifications were also made as to the information that the Financial Transactions and Reports Analysis Centre (FINTRAC) may receive, collect or disclose, and expands the circumstances in which the agency (or the Canada Border Services Agency) can disclose information received or collected under the Act. It also updates the review and appeal provisions related to cross-border currency reporting and brings Part 1.1 of the Act into force.

[13] CSIS may also, in accordance with s.16 of the CSIS Act, collect foreign intelligence within Canada. However, these activities constitute a narrow scope of CSIS' mandate, which is largely focussed on investigating activities suspected of constituting threats to the security of Canada (in accordance with s.12) and conducting investigations to provide security assessments and advice (ss.13, 14, and 15).

[14] Measures include establishing record keeping and client identification requirements for financial services providers and other entities; requiring the reporting of suspicious financial transactions and of cross-border movements of currency and monetary instruments; and establishing an agency (Financial Transactions and Reports Analysis Centre) responsible for dealing with reported and other information.

7.0 Recent Developments

7.1 National Security Consultations

When former Bill C-51, the *Anti-terrorism Act* (ATA), was tabled in the House of Commons, many Canadians raised questions as to whether the proposed legislation appropriately safeguards both security and rights. As those concerns have not diminished since the passage of the ATA in 2015, the Prime Minister of Canada has charged the Minister of Public Safety and Emergency Preparedness, through a mandate letter, with priorities that include:

- "creation of a statutory committee of Parliamentarians with special access to classified information to review government departments and agencies with national security responsibilities"; and
- "work to repeal, in collaboration with the Minister of Justice, the problematic elements of Bill C-51 and introduce new legislation that strengthens accountability with respect to national security and better balances collective security with rights and freedoms".

7.2 In fulfilling these mandate commitments, the Government consulted Canadians on key elements of Canada's national security laws and policies to ensure they are effective at keeping Canadians safe, and equally reflect the rights, values and freedoms of Canadians. The consultations were anchored in *Our Security, Our Rights: National Security Green Paper, 2016*, and a detailed Background Document, which together provide an overview of ten key national security issues.[15] This consultation took place from September to December 2016, and included online responses to a questionnaire, email submissions, public town halls and online events, engagement with key stakeholders and academics, and parliamentary committee reviews.

7.3 As part of these consultations, the Government heard from subject matter experts, academics, security and intelligence officials, members of Parliament and senators, various civil society groups, as well as Canadians. Almost 60,000 responses to the online questionnaire and over 17,000 email responses were received. A public report on the results of the consultations is being developed for public release and summaries from the public town halls are available.[16] The Government is making the online and email submissions accessible through the Open Government portal.

7.4 The Government continues to analyze the input and will be using it to inform the further development of Canada's national security policies, and changes to laws and programs to ensure the effectiveness of the tools available to law enforcement and security agencies, while safeguarding Canadian rights and freedoms. The Minister of Public Safety and Emergency Preparedness has publicly stated his intention to table proposed changes to former Bill C-51.

7.5 *Security of Canada Information Sharing Act*

The *Security of Canada Information Sharing Act* (SCISA) was enacted in 2015 as part of the *Anti-terrorism Act*. It grants express, discretionary statutory authority for all federal institutions to disclose information, including personal information, to a limited number of federal institutions that are designated as recipients under the SCISA on the basis of their national security jurisdiction and responsibilities, provided that the information is relevant to that national security

[15] The ten key national security issues are: accountability, prevention, threat reduction, domestic national security information sharing, the Passenger Protect Program, *Criminal Code* terrorism measures, procedures for listing terrorist entities, terrorist financing, investigative capabilities in a digital world, and intelligence and evidence. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx

[16] Summaries of public town halls can be found at http://canada.ca/national-security-consultation

jurisdiction or those national security responsibilities. Under the SCISA, disclosure is made to the head of a designated recipient institution or their delegate(s).

7.6 The SCISA does not supersede or derogate from existing information disclosure authorities. Other statutory limits on the disclosure, the collection of information and general information management requirements apply to information disclosed under the SCISA. For example, requirements in the *Privacy Act* continue to apply to personal information disclosed pursuant to SCISA.

7.7 *Secure Air Travel Act, 2015*

In August 2015, the *Secure Air Travel Act* (SATA) came into force, which expanded the mandate of the Passenger Protect Program to allow the Minister of Public Safety and Emergency Preparedness to establish a list of individuals (the SATA List) when there are reasonable grounds to suspect they will engage or attempt to engage in an act that would threaten transportation security; and/or travel by air for the purpose of committing certain terrorism offences.

7.8 In addition, SATA authorizes the Minister to enter into written arrangements to share the SATA List, in whole or in part, with foreign partners. These arrangements are administrative in nature and not legally binding on either party. Information is shared in accordance with Canadian law, and safeguards are incorporated to protect privacy and establish limits on further use and disclosure.

8.0 Further Information and Reports

8.1 Further information about any aspect of this report may be requested from Charles Taillefer, Director, Privacy and Data Protection Policy Directorate, Digital Policy Branch, Innovation, Science and Economic Development Canada, 235 Queen Street, 1st Floor, Ottawa, Ontario, Canada K1A 0H5 (Charles.Taillefer@Canada.ca)

8.2 It is intended that future reports be provided at regular intervals. As this is the first such report, the Government welcomes feedback as to its format and usefulness. Future reports are expected to be considerably shorter given the time period addressed in this report.